



New Scams You Should Know About

While identity thieves still use old-school tricks like stealing wallets, digging through trash, or sending phishing emails, you've likely learned how to avoid those: protect your belongings, shred personal documents, and avoid clicking on suspicious links.

But as technology evolves, so do the tactics criminals use to steal your information. Here are some of the latest scams—and how to protect yourself.

Cryptocurrency Scams

Scammers are cashing in on the growing popularity of Bitcoin and other cryptocurrencies. Common schemes include:

- **Blackmail:** Scammers claim to have embarrassing information or evidence and demand payment in cryptocurrency to keep quiet.
- **Referral chains:** These work like digital pyramid schemes—you're promised profit if you recruit others, but first you must pay to join.
- **Fake investment pitches:** Fraudsters promise big returns in exchange for an upfront investment in cryptocurrency.

How to stay safe:

Research any person, company, or opportunity before investing. Don't fall for pressure tactics or urgent payment demands. Report cryptocurrency fraud to your local police, the FBI, and the FTC at reportfraud.ftc.gov.

Skimming

Skimming involves devices that secretly read the magnetic strip on your credit or debit card—often placed at gas pumps, ATMs, or even used by dishonest staff in retail and restaurants.

How to stay safe:

Inspect card readers for anything loose or unusual. Avoid using machines that look tampered with. At restaurants, take your card to the register rather than handing it off.

Shimming

Shimming is a newer scam targeting chip cards. A thin device called a “shim” is inserted into a card reader slot. When you insert your chip card, it captures your card’s data, which can be used to make counterfeit cards with magnetic stripes.

How to stay safe:

Use machines in well-lit, busy areas or indoors. Consider switching to contactless payments like Apple Pay® or Google Pay™ for extra security.

Fake Tech Support Calls

Scammers pose as tech support from Microsoft or other companies, claiming your computer is infected. They’ll direct you to a fake website that “removes” viruses while secretly installing malware.

How to stay safe:

Hang up—real tech companies won’t call you out of the blue. Don’t click on pop-ups telling you to call a number. Instead, contact your device manufacturer or trusted tech support directly. Always keep your software and antivirus programs updated.

Tax Refund Fraud

Identity thieves sometimes file fake tax returns using stolen personal information to claim refunds. Victims may only learn about the scam when the IRS notifies them of duplicate filings—or they may get phishing emails claiming their tax info is incomplete.

How to stay safe:

The IRS never contacts people by email to request personal info. Watch for official notices about multiple filings or wages from unknown employers—these are red flags. If you suspect fraud, contact the IRS immediately.

Final Tips

- Never give out personal information by phone or email to unsolicited contacts.
- Don't click on links in emails. Instead, type the company's website address directly into your browser.
- If you get a suspicious call or message, hang up and contact the company using a verified phone number.

Sources: TIME: Moneyland, FTC.gov, AARP